Transaction Monitoring and Auditing

ISACA – Houston Chapter

May 17, 2007

John Harrison

Managing Director

Protiviti, Inc.

In this Session…

- We will explore the largely untapped potential of transaction monitoring & auditing
- We will discuss, among other things:
  - Why this approach is gaining momentum
  - How transaction analysis can be used by management and auditors
  - How to get started
  - The use of transaction tools
  - Examples of interesting transaction types
  - Lessons learned

Defined

- For our purposes, *transaction monitoring* can be defined as any activity related to continuously examining a company's transactions for risk via:
  - data anomalies,
  - exceeded thresholds,
  - fluctuations,
  - and sensitive activities
- *Transaction auditing* assumes the same focus but may occur on a periodic or one-time basis

Historical Background

- Some Computer Assisted Audit Techniques (CAATs) have been used for over a decade
- Continuous Control Monitoring has been an academic emphasis for years
- Certain isolated data mining / business intelligence initiatives have been conducted
- Some SOX testers have performed 100% tests using automated queries

Why now?

- There are a number of forces converging that is making this a top-of-mind topic
  - 80% of CFOs say that the costs of SOX have outweighed the benefits
  - Recent changes from the PCAOB and SEC allow for fresh risk-based coverage alternatives
  - Transaction monitoring can provide a non-intrusive, self-documenting technique that can also provide benefits beyond compliance

Why now?

- Audit shops are shifting back to forensics
  - Looking to add more value than simple pass/fail compliance testing
  - There is increased interest in fraud
- Management is looking for more frequent and real time indicators of risk
- Enterprise Risk Management is firming up
- Emerging technologies are making continuous monitoring more practical

What are some scenarios?

- Internal Audit annually tests for risk anomalies and fraud indicators, but over 100% of the population
- SOX tests use automated transaction analysis or rely on management's monitoring processes instead of manual sample tests
- Management calculates the "real" impact of a deficiency by looking over the whole year of data

What are some scenarios?

- Process Owners alerted to critical unexpected events real-time
- Control owners receive focused data to monitor and continually improve their areas
- Certifiers consider substantiated risk indicators each quarter for their 302 assertions

So where should I start?

- Look for value
  - Start with something that has potential for an immediate and relatable impact (prove the concept)
  - Opportunity for potential big bottom line results
  - Items that are significant within the risk-based, top-down prioritization
  - Controls that are time consuming and expensive to test manually

So where should I start?

- Look for value
  - Areas of past issues
  - Areas more prone to fraud
  - Business rules that should be consistently followed, but can't be systematically enforced

So where should I start?

- Look for easy
  - Some of the tools available have pre-built queries/rules that map to common systems
  - Preferably the data is in one system
  - The system should allow for easy and repeated access to the data

So where should I start?

- Look for easy
  - Avoid business rules or patterns that are overly complex to interpret or conclude on
    - Start with something that is relatively simple and straightforward
  - Helpful if previously manually conducted at least once (designed/proved out)

Tools are making it happen

- Data Mining / Business Intelligence
  - ACL, IDEA, Oversight, Cognos, Business Objects, etc.
- Integrated ERP GRC Modules
  - SAP GRC (formerly Virsa), Oracle GRC, etc.
- 3rd Party ERP Products
  - Approva, Logical Apps, D2C, etc.
- Database
  - Oracle Audit Vault, Lumigent, etc.
- Native exception/edit reports & Custom Reports

Interesting Transaction Types

Ex's of Master Data Anomalies / Fraud Indicators

General	Duplicate, incomplete, or obsolete records
Asset	Unusual useful lives compared to asset class
Customer	Credit limits do not adequately correlate with credit ratings
Employee	Invalid SSN, Invalid Address
Vendor	Multiple changes within period (manipulating and then covering tracks)

Interesting Transaction Types

Master Data Integrity	Duplicates	Missing
Asset	Description, location, serial number	Description, location, asset class, serial #
Customer	Name, bank account, address, telephone #	Customer name, address, phone, zip
Employee	Name, Address, bank account	Name, address, SSN, telephone #, Zip, dept.
Vendor	Name, address, telephone #	Name, address, Telephone #, Zip

Interesting Transaction Types

Ex's of Master Data Anomalies / Fraud Indicators

Vendor

- Vendor address matches employee address
- Vendor bank account matches employee bank account
- Multiple changes within period (manipulating and then covering tracks)
- With only post office box
- No activity since ___

Interesting Transaction Types

Unauthorized Activity

(Conducted by someone outside of expected authorized group)

- Asset Updates
- Vendor Updates
- Employee Updates
- Security Updates
- Program / Configuration Updates

Interesting Transaction Types

Segregation of Duty Exploitation

- Accountant approving/posting their own journal entries
- The same person creating a vendor & paying that vendor
- Creating a fictitious customer and processing credit memos
- IT entry or edits of production data

Interesting Transaction Types

Transaction Checks

- Vendor payments to an employee's bank account or address
- Invoice amounts – Benford's Law analysis
- Duplicate payments – invoice date, invoice #, amount, vendor name
- Payment terms on invoice different than terms on vendor record
- Concurrent system usage compared to purchased software licenses

Interesting Transaction Types

Transaction Checks (cont…)

- Post close entries
- System balancing (interface matching)
- Unusually large payments
- Repeating payments to “one-time” vendors
- Payments without an invoice reference

Lessons Learned

- Don’t expect to monitor the world
  - Let risk significance and potential benefits drive a rational phased roll-out
- Don’t underestimate the time it takes to do this right
  - aligning the people
  - understanding the data
  - building in a sustainable response plan

Lessons Learned

- Get a multi-disciplined team committed
  - IT, Business, Audit involved in definition
  - Define who will own the output (who responds)
- Must define specific enough criteria to produce a reasonably filtered list
  - Otherwise, owners will simply ignore or neglect other important responsibilities

Lessons Learned

- Carefully tailor default rules to your environment / data
  - don’t assume out-of-the box queries and reports will immediately provide what you need
- Check and double-check the assumptions
  - For proper use of the source data
  - And rational interpretation of the results

Thank you!

For More Information:

John Harrison

Managing Director

Protiviti, Inc.

john.harrison@protiviti.com

(713) 314-4996